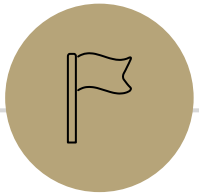
Number Theory Cont.

CSE 311: Foundations of Computing I
Lecture 10

Announcements

- HW2 solutions and Number Theory Reference Sheets are at the front
- HW3 is due tonight at 11:59 pm



Review

Modular Arithmetic

Divides

For integers a, b, we say $a \mid b$ ("a divides b") iff there exists some integer k such that $b = ka$.

5 | 25 -3 | 9 7 ∤ 22

Division Theorem

For any integer a and positive integer d, there exist unique integers q, r with $0 \leq r < d$ such that $a = qd + r$.

Congruence

For integers a, b and positive integer m, we say $a \equiv_m b$ iff $m \mid (a - b)$.

a%m = b%m

Notation

We will work with the notation $a \equiv_m b$.

$$(19 + 33) \cdot 5 \equiv_{10} 52 \cdot 5 \equiv_{10} 260 \equiv_{10} 0$$

In practice, you'll often see the notation $a \equiv b \pmod{m}$.

$$(19 + 33) \cdot 5 \equiv 52 \cdot 5 \equiv 260 \equiv 0 \pmod{10}$$

Properties of Mod

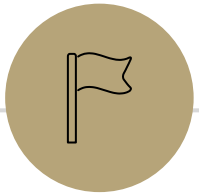
Let a, b, c, d and $m > 0$ be integers.

- If $a \equiv_m b$, then $b \equiv_m a$.
- If $a \equiv_m b$ and $c \equiv_m d$, then $a + c \equiv_m b + d$.
- If $a \equiv_m b$ and $c \equiv_m d$, then $ac \equiv_m bd$.
- If $a \equiv_m b$ and $b \equiv_m c$, then $a \equiv_m c$.

$x \equiv_{10} 2$

$y \equiv_{10} 5$

$xy \equiv_{10} 10 \equiv_{10} 0$



Modular Arithmetic Proofs

Prove or Disprove

Definition
$a \mid b \coloneqq \exists k \in \mathbb{Z}\,(b = ka)$

f Claim 1: For integers a, b, c if $b \mid a$ and $c \mid a$ then $bc \mid a$.

T Claim 2: For integers a, b, c if $a \mid b$ and $a \mid c$ then $a \mid bc$.

Poll Everywhere
pollev.com/anjalia

Prove or Disprove

Definition
$a \mid b \coloneqq \exists k \in \mathbb{Z}\,(b = ka)$

Claim 1: For integers a, b, c if $b \mid a$ and $c \mid a$ then $bc \mid a$.

This claim is false. Consider $a = 12$, $b = 6$, $c = 4$.
Then $b \mid a$ and $c \mid a$ but $bc \nmid a$.
This is a counterexample to the claim.

Prove or Disprove

Definition
$a \mid b \coloneqq \exists k \in \mathbb{Z}\,(b = ka)$

Claim 2: For integers a, b, c if $a \mid b$ and $a \mid c$ then $a \mid bc$.

Let a, b, c be arbitrary integers. Suppose a | b and a | c. By def of divides, there exist integers j, k such that b = ak and c = aj. Consider bc:

$$bc = (ak)(aj) = a(akj)$$

Since a, k, j are integers, akj is an integer. So a | bc.

Since a, b, c were arbitrary, the claim holds.

For integers a, b and $m > 0$, $a \equiv_m b$ if and only if $a \,\%\, m = b \,\%\, m$

$\Rightarrow$ Let $a, b, m > 0$ be arbitrary integers. Suppose $a \equiv_m b$. So $m \mid (a-b)$. So there exists some integer k such that $a - b = mk$. So $a = mk + b$. By the Division Theorem, $a = qm + (a \,\%\, m)$ for some integer q, and $0 \le a \,\%\, m < m$. So:

$$mk + b = qm + (a \,\%\, m)$$
$$b = qm - km + (a \,\%\, m)$$
$$b = (q-k)m + (a \,\%\, m)$$

$b = sm + r$, $r = b \,\%\, m$, $0 \le r < m$

By the Division Theorem, we have $a \,\%\, m = b \,\%\, m$.

Since a, b, m were arbitrary, the claim holds.

$m \mid (a-b) \iff mx = a-b$

For integers a, b and $m > 0$, $a \equiv_m b$ if and only if $a \,\%\, m = b \,\%\, m$.

$\Leftarrow$ Let $a, b, m > 0$ be arbitrary integers. Suppose $a\%m = b\%m$.
By Division Theorem, $a = mq + (a\%m)$ for some integer q and $b = ms + (b\%m)$ for some integer s. Consider $a-b$:

$$\begin{aligned} a-b &= mq + (a\%m) - (ms + (b\%m)) \\ &= mq - ms + (a\%m) - (b\%m) \\ &= m(q-s) \end{aligned}$$

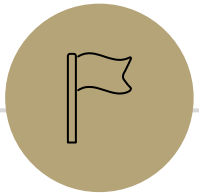
Since $a\%m = b\%m$

since q, s are integers, $q-s$ is an integer. So $m \mid (a-b)$.
So $a \equiv_m b$ since a, b, m were arbitrary, the claim holds.

Summary: Properties of Mod

Let a, b, c, d and $m > 0$ be integers.

- If $a \equiv_m b$, then $b \equiv_m a$.
- If $a \equiv_m b$ and $c \equiv_m d$, then $a + c \equiv_m b + d$.
- If $a \equiv_m b$ and $c \equiv_m d$, then $ac \equiv_m bd$.
- If $a \equiv_m b$ and $b \equiv_m c$, then $a \equiv_m c$.
- $a \equiv_m b$ if and only if $a \,\%\, m = b \,\%\, m$.



Primes & GCD

Prime and Composite

2, 3, 5, 7, 11, 13, ...

Definition:

An integer $p > 1$ is prime iff its only positive divisors are 1 and p.

An integer $p > 1$ is composite iff it is not prime.

Greatest Common Divisor

$\frac{99}{18} = \frac{11}{2}$

Definition:

The Greatest Common Divisor of integers a and b (denoted $\gcd(a, b)$) is

the largest integer c such that $c \mid a$ and $c \mid b$

For Example:

$\gcd(99,18) =$ 9

$\gcd(100, 125) =$ 25

$\gcd(7,11) =$ 1

$\gcd(13,0) =$ 13

Calculating the GCD: Approach 1

Fundamental Theorem of Arithmetic: Every positive integer greater than 1 has a unique prime factorization.

$100 = 2 \cdot 2 \cdot 5 \cdot 5$ $72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$

Approach 1 to finding $\gcd(a, b)$:

- Find the prime factorization of a
- Find the prime factorization of b
- Identify all common prime factors.
- Multiply the common prime factors together. 4
  This is the GCD. (4)

$\gcd(100, 72)$

$100 = 2 \cdot 2 \cdot 5 \cdot 5$

$72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$

VERY INEFFICIENT

Calculating the GCD: Approach 2

Claim: For positive integers a, b, $gcd(a, b) = gcd(b, a\%b)$

For example:

$= gcd(6, 4)$

$gcd(110, 30) = gcd(30, 20)$

$= gcd(20, 10)$

$= gcd(10, 0)$

$= 10$

We'll prove this in a minute. But first: how can we use this fact to devise an algorithm for computing $\mathbf{gcd}(a, b)$?

Calculating the GCD: Approach 2

Euclid's Algorithm. To find $\mathbf{gcd}(a, b)$:

- Repeatedly use $\mathbf{gcd}(a, b) = \mathbf{gcd}(b, a \,\%\, b)$ to reduce numbers
- Stop once you reach $\mathbf{gcd}(g, 0)$. Return g.

For Example:

$\mathbf{gcd}(660,126) =$ gcd(126, 30)

= gcd(30, 6)

= gcd(6, 0)

= 6

Euclid’s Algorithm in Java

Proof of Claim

Claim: For positive integers a, b, $\gcd(a, b) = \gcd(b, a \,\%\, b)$.

How do you show that two GCDs are equal?

- First consider some arbitrary common divisor of a and b, call it d. Prove d is a common divisor of b and a%b.
- Then consider some arbitrary common divisor of b and a%b, call it d. Prove d is a common divisor of a & b
- Then their GCDs are the same.

Claim: For positive integers a, b, $\gcd(a, b) = \gcd(b, a \,\%\, b)$.

Let a, b be arbitrary positive integers. By Division Theorem, $a = qb + (a \,\%\, b)$ for some integer q.

Let d be arbitrary and suppose $d \mid b$ and $d \mid a \,\%\, b$. We aim to show $d \mid a$. By def of divides, $b = dk$ and $a \,\%\, b = dj$ for some integers j, k. Observe:

$$a = qb + (a \,\%\, b) = q(dk) + (dj) = d(qk + j)$$

since q, k, j are ints $qk + j$ is an int. so $d \mid a$.

Suppose $d \mid a$ and $d \mid b$. Then $a = dm$ and $b = dn$ for some int m, n.

$$a \,\%\, b = a - qb = dm - qdn = d(m - qn)$$

Since m, q, n are ints, $m - qn$ is an int so $d \mid a \,\%\, b$.

So a, b have the same common divisors as $b, a \,\%\, b$. Thus they have the same GCD: $\gcd(a, b) = \gcd(b, a \,\%\, b)$.